Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - aeNovo SQL Injection or Cross-Site Scripting
  - aspReady FAQ Manager SQL Injection
  - GFI MailSecurity Arbitrary Code Execution or Denial of Service
  - Hauri Arbitrary Code Execution
  - **MailEnable Arbitrary Code Execution (Updated)**
  - Microsoft Client Service for NetWare Arbitrary Code Execution
  - Microsoft Collaboration Data Objects Arbitrary Code Execution
  - Microsoft DirectX DirectShow Arbitrary Code Execution
  - Microsoft Internet Explorer Arbitrary Code Execution
  - Microsoft Network Connection Manager Denial of Service
  - Microsoft Windows FTP Client Arbitrary File Control
  - Microsoft Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service
  - Microsoft Windows Plug and Play Arbitrary Code Execution
  - Microsoft Windows Shell Arbitrary Code Execution
  - Microsoft Windows XP Wireless Zero Configuration Service Information Disclosure
  - WinRAR Arbitrary Code Execution
  - **Symantec Anti Virus Arbitrary Code Execution (Updated)**
  - Webroot Desktop Firewall Authentication Bypassing or Arbitrary Code Execution
- UNIX / Linux Operating Systems
  - **Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass (Updated)**
  - **Arc Insecure Temporary File Creation (Updated)**
  - **Bacula Insecure Temporary File Creation (Updated)**
  - Cyphor Cross-Site Scripting & SQL Injection
  - Debian Linux Firewall Loading Failure
  - **GNU CPIO CHMod File Permission Modification (Updated)**
  - **GNU CPIO Directory Traversal (Updated)**
  - **GNU Texinfo Insecure Temporary File Creation (Updated)**
  - Graphviz Insecure Temporary File Creation
  - Hiki Multiple Cross-Site Scripting
  - **HylaFAX Insecure Temporary File Creation (Updated)**
  - **Inter7 SqWebMail HTML Email Script Tag Script Injection (Updated)**
  - **Inter7 SqWebMail HTML Email Arbitrary Code Execution (Updated)**
  - Kaspersky Anti-Virus Engine Remote Buffer Overflow
  - KDE KOffice KWord RTF Remote Buffer Overflow
  - **LBL TCPDump Remote Denials of Service (Updated)**
  - **MasqMail Elevated Privileges (Updated)**
  - Mozilla Firefox IFRAME Handling Remote Denial of Service
  - **Multiple Vendors DIA Remote Arbitrary Code Execution (Updated)**
  - **Multiple Vendors Cfengine Insecure Temporary Files (Updated)**
  - **Perl 'rmtree()' Function Elevated Privileges (Updated)**
  - Multiple Vendors HylaFAX Insecure UNIX Domain Socket Usage
  - Multiple Vendors TCPDump BGP Decoding Routines Denial of Service
  - **Multiple Vendors RealNetworks RealPlayer & Helix Player Format String**
  - **Multiple Vendors Squid NTLM Authentication Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel 64 Bit PTrace Kernel Memory Access (Updated)**
  - **Multiple Vendors Linux Kernel XFRM Array Index Buffer Overflow (Updated)**
  - **Multiple Vendors Linux Kernel 'ptrace()' Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel 'MMap()' Denial of Service (Updated)**
  - **Multiple Vendors GDB Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel 64 Bit 'AR-RSC' Register Access (Updated)**
  - **Multiple Vendors Linux Kernel EXT2/EXT3 File Access Bypass (Updated)**
  - **Multiple Vendors Linux Kernel 'Ipt_recent' Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel IPSec Policies Authorization Bypass (Updated)**
  - Multiple Vendors Linux Kernel Denial of Service & Information Disclosure
  - Multiple Vendors Linux Kernel USB Subsystem Denials of Service
  - Multiple Vendors Linux Kernel Denials of Service
  - **Multiple Vendors Linux Kernel Management Denials of Service (Updated)**

- **Multiple Vendor LibTiff Tiff Image Header Remote Denial of Service (Updated)**
- Multiple Vendors OpenSSL Insecure Protocol Negotiation
- **Multiple Vendors Kerberos V5 Multiple Vulnerabilities (Updated)**
- **Multiple Vendors Util-Linux UMount Remounting Filesystem Elevated Privileges (Updated)**
- Multiple Vendors CDDB Client Format String
- **Net-SNMP Protocol Denial Of Service (Updated)**
- **Net-SNMP Fixprox Insecure Temporary File Creation (Updated)**
- OpenVMPS Logging Function Format String
- **Paul Vixie Cron Crontab Information Disclosure (Updated)**
- PHPMyAdmin File Include
- SGI IRIX 'runpriv' Input Validation
- **Shorewall MACLIST Firewall Rules Bypass (Updated)**
- **slocate Long Path Denial of Service (Updated)**
- Sun Directory Server Remote Arbitrary Code Execution
- SUSE Linux PowerSave Daemon Denial of Service
- **SuSE YaST Buffer Overflow (Updated)**
- SuSE YaST Package Repositories Insecure Permissions
- SUSE Linux Elevated Privileges
- SUSE ResMgr Unauthorized USB Device Access
- **UW-imapd Denial of Service and Arbitrary Code Execution (Updated)**
- up-imapproxy Format String
- **Webmin / Usermin Remote PAM Authentication Bypass (Updated)**
- **Weex Format String (Updated)**
- Xloadimage NIFF Image Buffer Overflow
- **Ruby Safe Level Restrictions Bypass (Updated)**
- Zeroblog Cross-Site Scripting
- Zope 'RestructuredText' Unspecified Security Vulnerability

- Multiple Operating Systems
  - Accelerated E Solutions SQL Injection
  - PHP Advanced Transfer Cross-Site Scripting
  - BEA WebLogic Server & WebLogic Express Multiple Vulnerabilities
  - **Ethereal Denial of Service or Arbitrary Code Execution (Updated)**
  - **HP OpenView Event Correlation Services Remote Elevated Privileges (Updated)**
  - IBM Tivoli Monitoring Web Health Console Multiple Denial of Service
  - **Py2Play Object Remote Python Code Execution (Updated)**
  - MediaWiki Database Corruption
  - MediaWiki HTML Inline Style Attributes Cross-Site Scripting
  - **SquirrelMail Cross-Site Scripting (Updated)**
  - **Mozilla Browser/Firefox Arbitrary Command Execution (Updated)**
  - **Mozilla Suite And Firefox DOM Property Overrides (Updated)**
  - **Mozilla/Netscape/Firefox Browsers Domain Name Buffer Overflow (updated)**
  - **Mozilla Suite And Firefox Wrapped 'javascript:' URLs (Updated)**
  - **Mozilla Browser / Firefox Multiple Vulnerabilities (Updated)**
  - **Multiple Vendor Telnet Client Information Disclosure (Updated)**
  - Multiple Vendor Antivirus Products Malformed Archives Scan Bypass
  - **Multiple Vendors PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution (Updated)**
  - **Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service (Updated)**
  - MyBloggie SQL Injection
  - **MySQL 'mysql_install_db' Insecure Temporary File Creation (Updated)**
  - **MySQL User-Defined Function Buffer Overflow (Updated)**
  - Novell NetMail NMAP Agent Remote Buffer Overflow
  - **OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials (Updated)**
  - **OpenVPN Multiple Remote Denials of Service (Updated)**
  - OScommerce SQL Injection
  - **PHP-Fusion Multiple SQL Injection (Updated)**
  - Planet Technology FGSW-2402RS Switch Backdoor Password
  - Sun Java System Application Server Java Server Page Information Disclosure
  - TellMe Cross-Site Scripting & Information Disclosure
  - Utopia News Pro Cross-Site Scripting & SQL Injection
  - VERITAS NetBackup Java User-Interface Remote Format String
  - versatileBulletinBoard Cross-Site Scripting, SQL Injection, & Information Disclosure
  - W3C Libwww Multiple Unspecified Vulnerabilities

Wireless

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
aeNovo aeNovo, aeNovoShop, aeNovoWYSI	Multiple input validation vulnerabilities have been reported in aeNovo, aeNovoShop, and aeNovoWYSI that could let remote malicious users perform SQL injection or Cross-Site Scripting. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	aeNovo SQL Injection or Cross-Site Scripting	Medium	Security Focus, ID: 15036, 15038, October 7, 2005
aspReady FAQ Manager	An input validation vulnerability has been reported in aspReady FAQ Manager that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	aspReady FAQ Manager SQL Injection	Medium	Security Tracker, Alert ID: 1015015, October 6, 2005
GFI MailSecurity GFI MailSecurity for Exchange/ SMTP 8.1	A buffer overflow vulnerability has been reported in GFI MailSecurity that could let remote malicious users execute arbitrary code or cause a Denial of Service. A vendor patch is available: ftp://ftp.gfi.com/patches/MSEC8_PATCH_20050919_01.zip Currently we are not aware of any exploits for this vulnerability.	GFI MailSecurity Arbitrary Code Execution or Denial of Service	High	Security Focus, ID 15081, October 11, 2005
Hauri vrAZMain.dll 5.8.22.137 in ViRobot Expert 4.0, ViRobot Advanced Server, LiveCall	A buffer overflow vulnerability has been reported in vrAZMain.dll 5.8.22.137 utilized in ViRobot Expert 4.0, ViRobot Advanced Server, LiveCall, ALZ archive processing, that could let remote malicious users execute arbitrary code. Vendor upgrade, vrAZMain.dll 5.9.22.154, available via online update. Currently we are not aware of any exploits for this vulnerability.	Hauri Arbitrary Code Execution	High	Secunia, Advisory: SA16852, October 6, 2005
MailEnable Enterprise 1.1, Professional 1.6	A buffer overflow vulnerability has been reported in MailEnable that could let remote malicious users execute arbitrary code. Vendor hotfix available: http://www.mailenable.com/hotfix/ **An exploit has been published.**	MailEnable Arbitrary Code Execution CAN-2005-3155	High	Secunia, Advisory: SA17010, October 4, 2005 **Security Focus, ID: 15006, October 7, 2005**
Microsoft Client Service for NetWare	A buffer overflow vulnerability has been reported in Client Service for NetWare that could let malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-046.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Client Service for NetWare Arbitrary Code Execution CAN-2005-1985	High	Microsoft, Security Bulletin MS05-046, October 11, 2005

Microsoft Collaboration Data Objects	A buffer overflow vulnerability has been reported in Collaboration Data Objects that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-048.mspx A Proof of Concept exploit script has been published.	Microsoft Collaboration Data Objects Arbitrary Code Execution CAN-2005-1987	High	Microsoft, Security Bulletin MS05-048, October 11, 2005 USCERT, VU#883460 Technical Cyber Security Alert TA05-284A, October 11, 2005
Microsoft DirectX DirectShow 7.0 to 9.0c	A buffer overflow vulnerability has been reported in DirectX DirectShow that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft DirectX DirectShow Arbitrary Code Execution CAN-2005-2128	High	Microsoft, Security Bulletin MS05-050, October 11, 2005 USCERT, VU#995220 Technical Cyber Security Alert TA05-284A, October 11, 2005
Microsoft Internet Explorer 5.01, 5.5, 6.0	A vulnerability has been reported in Internet Explorer that could let remote malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-052.mspx An exploit has been published.	Microsoft Internet Explorer Arbitrary Code Execution CAN-2005-2127	High	Microsoft, Security Bulletin MS05-052, October 11, 2005 Technical Cyber Security Alert TA05-284A, October 11, 2005
Microsoft Network Connection Manager	A vulnerability has been reported in Network Connection Manager that could let malicious users cause a Denial of Service. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-045.mspx An exploit has been published.	Microsoft Network Connection Manager Denial of Service CAN-2005-2307	Low	Microsoft Security Bulletin MS05-045, October 11, 2005
Microsoft Windows FTP Client	An input validation vulnerability has been reported in Windows FTP Client that could let remote malicious users to obtain arbitrary file control. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-044.mspx A Proof of Concept exploit script has been published.	Microsoft Windows FTP Client Arbitrary File Control CAN-2005-2126	Medium	Microsoft, Security Bulletin MS05-044, October 11, 2005
Microsoft Windows Microsoft Distribution Transaction Coordinator (MSDTC) and COM+	A buffer overflow vulnerability has been reported in Windows MSDTC and COM+ that could let local or remote malicious users execute arbitrary code, obtain elevated privileges or cause a Denial of Service. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-051.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows MSDTC and COM+ Privilege Elevation, Arbitrary Code Execution, or Denial of Service CAN-2005-1978 CAN-2005-1979 CAN-2005-1980 CAN-2005-2119	High	Microsoft, Security Bulletin MS05-051, October 11, 2005 US-CERT VU#180868, US-CERT VU#950516 Technical Cyber Security Alert TA05-284A, October 11, 2005
Microsoft Windows Plug and Play	A buffer overflow vulnerability has been reported in Windows Plug and Play that could let malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-047.mspx Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Plug and Play Arbitrary Code Execution CAN-2005-2120	High	Microsoft, Security Bulletin MS05-047, October 11, 2005 USCERT, VU#214572 Technical Cyber Security Alert TA05-284A, October 11, 2005
Microsoft Windows Shell	A vulnerability has been reported in Windows Shell that could let malicious users execute arbitrary code. Vendor fix available: http://www.microsoft.com/technet/security/Bulletin/MS05-049.mspx Currently we are not aware of any exploits for this	Microsoft Windows Shell Arbitrary Code Execution CAN-2005-2117 CAN-2005-2118 CAN-2005-2122	High	Microsoft, Security Bulletin MS05-049, October 11, 2005 USCERT, VU#922708 Technical Cyber Security Alert

	vulnerability.			TA05-284A, October 11, 2005
Microsoft Windows XP Wireless Zero Configuration Service	A vulnerability has been reported in Windows XP Wireless Zero Configuration Service that could let remote malicious users disclose information. No workaround or patch available at time of publishing. There is no exploit code required.	Microsoft Windows XP Wireless Zero Configuration Service Information Disclosure	Medium	Security Focus, ID: 15008, October 4, 2005
RarLab WinRar prior to 3.51	Multiple vulnerabilities have been reported in WinRar that could let remote malicious users to execute arbitrary code. Upgrade to newest version: http://www.rarlabs.com/download.htm Currently we are not aware of any exploits for this vulnerability.	WinRAR Arbitrary Code Execution	High	Secunia, Advisory: SA16973, October 11, 2005
Symantec Symantec AntiVirus Scan Engine 4.0, 4.3	A buffer overflow vulnerability has been reported in Symantec AntiVirus that could let remote malicious users execute arbitrary code. Vendor upgrade available: http://securityresponse.symantec.com/avcenter/security/Content/2005.10.04.html#savse4-3-12 Currently we are not aware of any exploits for this vulnerability.	Symantec Anti Virus Arbitrary Code Execution CAN-2005-2758	High	Symantec Security Response, SYM05-017, October 4, 2005 **USCERT, VU#849209**
Webroot Software Inc. Webroot Desktop Firewall 1.3.0.43	Multiple vulnerabilities have been reported in Webroot Desktop Firewall that could let local malicious users bypass authentication or execute arbitrary code. Upgrade to version 1.3.0.5.2 using the applications 'Check for Updates' functionality. Currently we are not aware of any exploits for these vulnerabilities.	Webroot Desktop Firewall Authentication Bypassing or Arbitrary Code Execution	High	Security Focus, ID; 15016, October 6, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Apache Software Foundation Apache 2.0.x	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyCLient optional' directive, which could let a remote malicious user bypass security policies. Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ SGI: ftp://oss.sgi.com/projects/sgi_propack/	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CAN-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Debian Security Advisory, DSA 805-1, September 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005 Slackware Security Advisory, SSA:2005-251-02, September 9, 2005 Trustix Secure Linux

	download/3/updates/ Debian: http://security.debian.org/pool/updates/main/a/apache2/ Mandriva: http://www.mandriva.com/security/advisories Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Debian: http://security.debian.org/pool/updates/main/liba/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-12.xml Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-204.pdf Conectiva: ftp://atualizacoes.conectiva.com.br/10/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **HP:** **http://software.hp.com/** There is no exploit code required.			Security Advisory, TSLSA-2005-0047, September 9, 2005 Debian Security Advisory DSA 807-1, September 12, 2005 US-CERT VU#744929 Gentoo Linux Security Advisory, GLSA 200509-12, September 19, 2005 Avaya Security Advisory, ASA-2005-204, September 23, 2005 Conectiva Linux Announcement, CLSA-2005:1013, September 27, 2005 Turbolinux Security Advisory, TLSA-2005-94, October 3, 2005 **HP Security Bulletin, HPSBUX-01232, October 5, 2005**
ARC ARC 5.21 j	A vulnerability has been reported due to the insecure creation of temporary new archives by 'arc' and 'marc' before renamed to the user specified filename, which could let a malicious user obtain sensitive information. **Debian:** **http://security.debian.org/pool/updates/main/a/arc/** There is no exploit code required.	Arc Insecure Temporary File Creation CAN-2005-2945	Medium	Secunia Advisory: SA16805, September 16, 2005 **Debian Security Advisory, DSA 843-1, October 5, 2005**
Bacula Bacula 1.36 .3	Vulnerabilities have been reported in 'autoconf/randpass' and 'scripts/mtx-changer.in' due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files. The vulnerabilities have been fixed in the CVS repositories. **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	Bacula Insecure Temporary File Creation CAN-2005-2995	Medium	Secunia Advisory: SA16866, September 20, 2005 **SUSE Security Summary Report, SUSE-SR:2005:022, October 7, 2005**

Cyphor Cyphor 0.19	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'lostpwd.php' due to insufficient sanitization of the 'email' and 'nick' parameters and in 'newmsg.php' due to insufficient sanitization of the 'fid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'include/footer.php' due to insufficient sanitization of the 't_login' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proof of Concept exploits and an exploit script has been published.	Cyphor Cross-Site Scripting & SQL Injection	Medium	Security Focus, Bugtraq ID: 15049, October 10, 2005 Secunia Advisory: SA17104, October 10, 2005
Debian mason 0.13.92	A vulnerability has been reported in 'debian/postinst' due to a missing call to 'update-rc.d' after configuring mason, which could leave the system without a firewall and a false sense of security. Upgrade available at: http://security.debian.org/pool/updates/main/m/mason/mason_1.0.0-2.2_all.deb There is no exploit code required.	Debian Linux Firewall Loading Failure CAN-2005-3118	Medium	Debian Security Advisory, DSA 845-1, October 6, 2005
GNU cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6	A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions. Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-378.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32 Avaya: http://support.avaya.com/elmodocs2/	CPIO CHMod File Permission Modification CAN-2005-1111	Medium	Bugtraq, 395703, April 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 RedHat Security Advisory, RHSA-2005:378-17, July 21, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SCO Security Advisory, SCOSA-2005.32, August 18, 2005 Avaya Security Advisory, ASA-2005-191, September 6, 2005 Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005

	security/ ASA-2005-191.pdf Conectiva: ftp://atualizacoes. conectiva.com.br/10/ Ubuntu: http://security.ubuntu. com/ubuntu/pool/ main/c/cpio/ **Debian:** **http://security.debian. org/pool/updates/ main/c/cpio/** There is no exploit code required.			Ubuntu Security Notice, USN-189-1, September 29, 2005 **Debian Security Advisory, DSA 846-1, October 7, 2005**
GNU cpio 2.6	A Directory Traversal vulnerability has been reported when invoking cpio on a malicious archive, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo. org/glsa/glsa- 200506-16.xml Trustix: ftp://ftp.turbolinux.co.jp/ pub/TurboLinux/ TurboLinux/ Mandriva: http://www.mandriva. com/security/ advisories SCO: ftp://ftp.sco.com/pub/ updates/UnixWare/ SCOSA-2005.32 Avaya: http://support.avaya. com/elmodocs2/ security/ ASA-2005-191.pdf Conectiva: ftp://atualizacoes. conectiva.com.br/10/ Ubuntu: http://security.ubuntu. com/ubuntu/pool/ main/c/cpio/ **Debian:** **http://security.debian. org/pool/updates/ main/c/cpio/** A Proof of Concept exploit has been published.	CPIO Directory Traversal CAN-2005-1229	Medium	Bugtraq, 396429, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200506-16, June 20, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 SCO Security Advisory, SCOSA-2005.32, August 18, 2005 Avaya Security Advisory, ASA-2005-191, September 6, 2005 Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005 Ubuntu Security Notice, USN-189-1, September 29, 2005 **Debian Security Advisory, DSA 846-1, October 7, 2005**
GNU Texinfo 4.7	A vulnerability has been reported in 'textindex.c' due to insecure creation of temporary files by the 'sort_offline()' function, which could let a malicious user create/ overwrite arbitrary files. **Gentoo:** **http://security.gentoo. org/glsa/glsa- 200510-04.xml** **Mandriva:** **http://www.mandriva. com/security/**	GNU Texinfo Insecure Temporary File Creation CAN-2005-3011	Medium	Security Focus, Bugtraq ID: 14854, September 15, 2005 **Gentoo Linux Security Advisory, GLSA 200510-04, October 5, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:175, October 6, 2005** **Ubuntu Security Notice, USN-194-1,**

	advisories **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/t/texinfo/** There is no exploit code required.			**October 06, 2005**
Graphviz Graphviz 2.2.1	A vulnerability has been reported in '/dotty/dotty/dotty.lefty' due to the insecure creation of temporary files, which could let a malicious user overwrite arbitrary files. Update available at: http://www.graphviz.org/Download_source.php Debian: http://security.debian.org/pool/updates/main/g/graphviz/ There is no exploit code required.	Graphviz Insecure Temporary File Creation CAN-2005-2965	Medium	Debian Security Advisory, DSA 857-1, October 10, 2005
Hiki Hiki 0.8-0.8.2	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'login' link due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability has been reported due to an unspecified error when handling access to missing pages, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://hikiwiki.org/en/download.html There is no exploit code required.	Hiki Multiple Cross-Site Scripting CAN-2005-2336 CAN-2005-2803	Medium	Hiki Advisory, 2005-08-04, October 6, 2005
Hylafax Hylafax 4.2.1	Several vulnerabilities have been reported: a vulnerability was reported in the 'xferfaxstats' script due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability was reported because ownership of the UNIX domain socket is not created or verified, which could let a malicious user obtain sensitive information and cause a Denial of Service. Gentoo: http://security.gentoo.org/glsa/glsa-200509-21.xml **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	HylaFAX Insecure Temporary File Creation CAN-2005-3069 CAN-2005-3070	Medium	Security Focus, Bugtraq ID: 14907, September 22, 2005 Gentoo Linux Security Advisory, GLSA 200509-21, September 30, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:177, October 7, 2005**

Inter7 SqWebMail 5.0.4	A vulnerability has been reported because the '<script>' tag can be used in HTML comments, which could let a remote malicious user execute arbitrary code when malicious email is viewed. Patch available at: http://www.courier-mta.org/beta/sqwebmail/ Debian: http://security.debian.org/pool/updates/main/c/courier/ **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/courier/** There is no exploit code required; however, a Proof of Concept exploit has been published.	SqWebMail HTML Email Script Tag Script Injection CAN-2005-2820	Medium	Secunia Advisory: SA16704, September 6, 2005 Debian Security Advisory DSA 820-1, September 24, 2005 **Ubuntu Security Notice, USN-201-1, October 11, 2005**
Inter7 SqWebMail 5.0.4, 5.0 .1, 5.0.0, 4.0.5 -4.0.7, 4.0.4.20040524, 3.6.1, 3.6 .0, 3.5.0-3.5.3 , 3.4.1	A vulnerability has been reported due to insufficient sanitization of HTML emails, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://www.courier-mta.org/?download.php Debian: http://security.debian.org/pool/updates/main/c/courier **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/courier/** There is no exploit code required; however, a Proof of Concept exploit has been published.	SqWebMail HTML Email Arbitrary Code Execution CAN-2005-2724	Medium	Secunia Advisory: SA16600, August 29, 2005 Debian Security Advisory, DSA 793-1, September 1, 2005 **Ubuntu Security Notice, USN-201-1, October 11, 2005**
Kaspersky Labs Kaspersky Antivirus for Linux Servers 5.0.5, AntiVirus for Linux Workstations 5.0.5, Anti-Virus Personal 5.0.227; F-Secure Anti-Virus For Linux 4.5	A buffer overflow vulnerability has been reported in the scan engine when parsing a malformed 'CHM' file, which could let a remote malicious user execute arbitrary code. The vendor has released a signature update to address this issue. Users with updated signatures released after July 2005 are not vulnerable. Currently we are not aware of any exploits for this vulnerability.	Kaspersky Anti-Virus Engine Remote Buffer Overflow CAN-2005-2937	High	Security Focus, Bugtraq ID: 15054, October 10, 2005

KDE KOffice 1.4.1, 1.4, 1.3-1.3.5, 1.2.1, 1.2	A buffer overflow vulnerability has been reported when handling a malformed RTF file, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.koffice.org/download/ Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/ Currently we are not aware of any exploits for this vulnerability.	KDE KOffice KWord RTF Remote Buffer Overflow CAN-2005-2971	High	Security Focus, Bugtraq ID: 15060, October 11, 2005
LBL tcpdump 3.4 a6, 3.4, 3.5, alpha, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1 -3.8.3; IPCop 1.4.1, 1.4.2, 1.4.4, 1.4.5	Remote Denials of Service vulnerabilities have been reported due to the way tcpdump decodes Border Gateway Protocol (BGP) packets, Label Distribution Protocol (LDP) datagrams, Resource ReSerVation Protocol (RSVP) packets, and Intermediate System to Intermediate System (ISIS) packets. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-06.xml Mandriva: http://www.mandriva.com/security/advisories IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:10/tcpdump.patch Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-137 RHSA-2005-417 RHSA-2005-421.pdf TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE	LBL TCPDump Remote Denials of Service CAN-2005-1278 CAN-2005-1279 CAN-2005-1280	Low	Bugtraq, 396932, April 26, 2005 Fedora Update Notification, FEDORA-2005-351, May 3, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Ubuntu Security Notice, USN-119-1 May 06, 2005 Gentoo Linux Security Advisory, GLSA 200505-06, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:087, May 12, 2005 Security Focus, 13392, May 12, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:10, June 9, 2005 Avaya Security Advisory, ASA-2005-137, June 13, 2005 Turbolinux Security Advisory, TLSA-2005-63, June 15, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 13392, July 21, 2005 **Debian Security Advisory, DSA 850-1, October 9, 2005**

	F5: http://tech.f5.com/home/bigip/solutions/advisories/sol4809.html **Debian: http://security.debian.org/pool/updates/main/t/tcpdump/** Exploit scripts have been published.			
MasqMail MasqMail 0.2.18	Several vulnerabilities have been reported: a vulnerability was reported in the email address due to a sanitization error when the message fails to be sent, which could let a malicious user execute arbitrary commands with privileges of the mail user; and a vulnerability was reported when handling log files due to an unspecified error, which could let a remote malicious user overwrite arbitrary files. Mandriva: http://www.mandriva.com/security/advisories **Debian: http://security.debian.org/pool/updates/main/m/masqmail/** There is no exploit code required.	MasqMail Elevated Privileges CAN-2005-2662 CAN-2005-2663	Medium	Mandriva Linux Security Update Advisory, MDKSA-2005:168, September 20, 2005 **Debian Security Advisory, DSA 848-1, October 8, 2005**
Mozilla Firefox 1.0.7, 1.0.6	A remote Denial of Service vulnerability has been reported in the 'iframe' tag due to an error when handling overly large size attributes. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla Firefox IFRAME Handling Remote Denial of Service	Low	Security Tracker Alert ID: 1015011, October 6, 2005

Multiple Vendors DIA 0.91-0.94; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported in 'plug-ins/python/diasvg_ import.py' due to the insecure use of the 'eval()' function when handling a malicious Scalable Vector Graphics (SVG) file, which could let a remote malicious user execute arbitrary python code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/d/dia/ **Gentoo: http://security.gentoo.org/glsa/glsa-200510-06.xml** **SUSE: ftp://ftp.SUSE.com/pub/SUSE** **Debian: http://security.debian.org/pool/updates/main/d/dia/** A Proof of Concept exploit has been published.	DIA Remote Arbitrary Code Execution CAN-2005-2966	High	Security Focus, Bugtraq ID: 15000, October 3, 2005 Ubuntu Security Notice, USN-193-1, October 04, 2005 **Gentoo Linux Security Advisory, GLSA 200510-06, October 6, 2005** **SUSE Security Summary Report. SUSE-SR:2005:022, October 7, 2005** **Debian Security Advisory DSA, 847-1, October 8, 2005**
Multiple Vendors Cfengine 2.1.9, 2.1.8, 2.1.7 p1, 2.1 .0a9, 2.1.0a8, 2.1.0a6, 2.0.1-2.0.7 p1-p3, 2.0 .8p1, 2.0 .8, 2.0 .0, 1.6 a11, 1.6 a10, 1.5.3 -4, 1.5 x; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Several vulnerabilities have been reported: a vulnerability was reported in '/bin/cfmailfilter' and '/contrib/cfcron.in' due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files; and a vulnerability was reported in 'contrib/vicf.in/ due to the insecure creation of temporary files, which could let a remote malicious user create/overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/main/c/cfengine/ **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cfengine/** There is no exploit code required.	Cfengine Insecure Temporary Files CAN-2005-2960	Medium	Debian Security Advisories, DSA 835-1 & 836-1, October 1, 2005 **Ubuntu Security Notice, USN-198-1, October 10, 2005**

Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. A fixed version (5.8.4 or later) is available at: http://www.perl.com/CPAN/src/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Debian: http://security.debian.org/pool/updates/main/p/perl/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandrake: http://www.mandrakesecure.net/en/ftp.php HP: http://software.hp.com/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-196.pdf **RedHat: http://rhn.redhat.com/errata/RHSA-2005-674.html** Currently we are not aware of any exploits for this vulnerability.	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 Debian Security Advisory, DSA 696-1 , March 22, 2005 Turbolinux Security Advisory, TLSA-2005-45, April 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:079, April 29, 2005 HP Security Bulletin, HPSBUX01208, June 16, 2005 Secunia, Advisory: SA16193, July 25, 2005 Avaya Security Advisory, ASA-2005-196, September 13, 2005 **RedHat Security Advisory, RHSA-2005:674-10, October 5, 2005**
Multiple Vendors MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2, 10.1 x86_64, 10.1, MandrakeSoft Corporate Server 3.0 x86_64, 3.0, 2.1 x86_64, 2.1; Hylafax Hylafax 4.2.1	A vulnerability has been reported due to a failure to implement UNIX domain network communication securely, which could let a malicious user obtain sensitive information. Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.	Multiple Vendors HylaFAX Insecure UNIX Domain Socket Usage	Medium	Mandriva Linux Security Update Advisory, MDKSA-2005:177, October 7, 2005

Multiple Vendors RedHat Fedora Core3; LBL tcpdump 3.9.1, 3.9, 3.8.1-3.8.3, 3.7-3.7.2, 3.6.3, 3.6.2, 3.5.2, 3.5, alpha, 3.4, 3.4 a6	A remote Denial of Service vulnerability has been reported in the 'bgp_update_print()' function in 'print-bgp.c' when a malicious user submits specially crafted BGP protocol data. Update available at: http://cvs.tcpdump.org/cgi-bin/cvsweb/tcpdump/print-bgp.c Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tcpdump/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Slackware: ftp://ftp.slackware.com/pub/slackware IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id=35093&release_id=351848 IBM: http://www.ibm.com/support/ **Debian: http://security.debian.org/pool/updates/main/t/tcpdump/** A Proof of Concept exploit script has been published.	TCPDump BGP Decoding Routines Denial of Service CAN-2005-1267	Low	Security Tracker Alert, 1014133, June 8, 2005 Fedora Update Notification, FEDORA-2005-406, June 9, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0028, June 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:101, June 15, 2005 Fedora Update Notification, FEDORA-2005-407, June 16, 2005 Ubuntu Security Notice, USN-141-1, June 21, 2005 Turbolinux Security Advisory, TLSA-2005-69, June 22, 2005 Slackware Security Advisory, SSA:2005-195-10, July 15, 2005 Security Focus, Bugtraq ID: 13906, August 26, 2005 Security Focus, Bugtraq ID: 13906, October 3, 2005 **Debian Security Advisory, DSA 854-1, October 9, 2005**
Multiple Vendors RedHat Fedora Core4, Core3, Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; Real Networks RealPlayer For Unix 10.0.4, 10.0.3, RealPlayer 10 for Linux , Japanese, German, English, Helix Player for Linux 1.0-1.0.4	A format string vulnerability has been reported when displaying an invalid-handle error message, which could let a remote malicious user execute arbitrary code. RedHat: http://rhn.redhat.com/errata/RHSA-2005-788.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/	RealNetworks RealPlayer & Helix Player Format String CAN-2005-2710	High	RedHat Security Advisory, RHSA-2005:788-3, September 27, 2005 Fedora Update Notifications, FEDORA-2005-940 & 941, September 27, 2005 US-CERT VU#361181 Debian Security Advisory DSA 826-1, September 29, 2005 **Gentoo Linux Security Advisory, GLSA 200510-07, October 7, 2005**

	main/h/helix-player/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-07.xml** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** An exploit script has been published.			**SUSE Security Announcement, SUSE-SA:2005:059, October 10, 2005**
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE3-STABLE10, STABLE1	A remote Denial of Service vulnerability has been reported when handling certain client NTLM authentication request sequences. Upgrades available at: http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE11.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ Debian: http://security.debian.org/pool/updates/main/s/squid/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Squid NTLM Authentication Remote Denial of Service CAN-2005-2917	Low	Secunia Advisory: SA16992, September 30, 2005 Ubuntu Security Notice, USN-192-1, September 30, 2005 Debian Security Advisory, DSA 828-1, September 30, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:181, October 11, 2005**
Multiple Vendors SuSE Linux Enterprise Server 9, Linux 9.3 x86_64; Linux kernel 2.6.11, 2.6.8, 2.6.5	A vulnerability has been reported in 'ptrace' 64-bit platforms which could let a malicious user access kernel memory pages. SUSE: ftp://ftp.SUSE.com/pub/SUSE **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 64 Bit PTrace Kernel Memory Access CAN-2005-1763	Medium	SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. Patches available at: http://www.kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat:	Linux Kernel XFRM Array Index Buffer Overflow CAN-2005-2456	High	Security Focus, 14477, August 5, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005

	http://rhn.redhat.com/errata/RHSA-2005-663.html Mandriva: http://www.mandriva.com/security/advisories **RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.			**RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 amd64, 4.1 ia64; SuSE Linux 9.3 x86_64, 9.1 x86_64, 9.0 x86_64; Linux kernel 2.6.10, 2.6.8	A Denial of Service has been reported in 'ptrace()' due to insufficient validation of memory addresses. Updates available at: http://kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'ptrace()' Denial of Service CAN-2005-0756	Low	Ubuntu Security Notice, USN-137-1, June 08, 2005 SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **Multiple Vendors Linux Kernel 64 Bit 'AR-RSC' Register Access (Updated)**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6.10, 2.6.8	A vulnerability was reported has been reported in the 'mmap()' function because memory maps can be created with a start address after the end address, which could let a malicious user cause a Denial of Service or potentially obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'MMap()' Denial of Service CAN-2005-1265	Medium	Ubuntu Security Notice, USN-137-1, June 08, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Gentoo Linux; GNU GDB 6.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when loading malformed object files, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported which could let a malicious user obtain elevated privileges.	GDB Multiple Vulnerabilities CAN-2005-1704 CAN-2005-1705	High	Gentoo Linux Security Advisory, GLSA 200505-15, May 20, 2005 Turbolinux Security Advisory, TLSA-2005-68, June 22, 2005 RedHat Security Advisory,

	Gentoo: http://security.gentoo.org/glsa/glsa-200505-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gdb/ http://security.ubuntu.com/ubuntu/pool/main/b/binutils/ Mandriva: http://www.mandriva.com/security/advisories Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-659.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-673.html** **http://rhn.redhat.com/errata/RHSA-2005-709.html** Currently we are not aware of any exploits for these vulnerabilities.			RHSA-2005:659-9, September 28, 2005 **RedHat Security Advisory, RHSA-2005:673-5 & RHSA-2005:709-6, October 5, 2005**
Multiple Vendors Linux kernel 2.6 prior to 2.6.12.1	A vulnerability has been reported in the 'restore_sigcontext()' function due to a failure to restrict access to the 'ar.rsc' register, which could let a malicious user cause a Denial of Service or obtain elevated privileges. Updates available at: http://www.kernel.org/ SUSE: http://www.novell.com/linux/security/advisories/2005_44_kernel.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 64 Bit 'AR-RSC' Register Access CAN-2005-1761	Medium	Security Tracker Alert ID: 1014275, June 23, 2005 SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A vulnerability has been reported in the EXT2/EXT3 file systems, which could let a remote malicious user bypass access controls. Ubuntu: http://security.ubuntu.	Linux Kernel EXT2/EXT3 File Access Bypass CAN-2005-2801	Medium	Security Focus, Bugtraq ID: 14792, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005

	com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories **RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.			Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A remote Denial of Service vulnerability has been reported in the 'ipt_recent' module when specially crafted packets are sent. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories **RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Ipt_recent' Remote Denial of Service CAN-2005-2872	Low	Security Focus, Bugtraq ID: 14791, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Linux kernel 2.6.8-2.6.10, 2.4.21	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'msg_control' when copying 32 bit contents, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability was reported in the 'raw_sendmsg()' function, which could let a malicious user obtain sensitive information or cause a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html Mandriva: http://www.mandriva.com/security/advisories **RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of	Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service CAN-2005-2490 CAN-2005-2492	High	Secunia Advisory: SA16747, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Fedora Update Notifications, FEDORA-2005-905 & 906, September 22, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**

	any exploits for these vulnerabilities.			
Multiple Vendors Linux kernel 2.6-2.6.12.1	A vulnerability has been reported due to insufficient authorization before accessing a privileged function, which could let a malicious user bypass IPSEC policies. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ This issue has been addressed in Linux kernel 2.6.13-rc7. SUSE: ftp://ftp.SUSE.com/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-663.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPSec Policies Authorization Bypass CAN-2005-2555	Medium	Ubuntu Security Notice, USN-169-1, August 19, 2005 Security Focus, Bugtraq ID 14609, August 19, 2005 Security Focus, Bugtraq ID 14609, August 25, 2005 SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak in '/security/keys/request_key_auth.c;' a Denial of Service vulnerability was reported due to a memory leak in '/fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes when increasing the length, which could let a malicious user obtain sensitive information. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/testing/patch-2.6.14-rc4.bz2 There is no exploit code required.	Linux Kernel Denial of Service & Information Disclosure CAN-2005-3119 CAN-2005-3180 CAN-2005-3181	Medium	Secunia Advisory: SA17114, October 12, 2005
Multiple Vendors Linux kernel 2.6-2.6.14	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported when handling asynchronous USB access via usbdevio; and a Denial of Service vulnerability was reported in the 'ipt_recent.c' netfilter module due to an error in jiffies comparison. **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-514.html** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel USB Subsystem Denials of Service CAN-2005-2873 CAN-2005-3055	Low	Secunia Advisory: SA16969, September 27, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Linux Kernel 2.6-2.6.14	Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'sys_set_mempolicy' function when a	Multiple Vendors Linux Kernel Denials of Service	Low	Ubuntu Security Notice, USN-199-1, October 10, 2005

	malicious user submits a negative first argument; a Denial of Service vulnerability was reported when threads are sharing memory mapping via 'CLONE_VM'; a Denial of Service vulnerability was reported in 'fs/exec.c' when one thread is tracing another thread that shares the same memory map; a Denial of Service vulnerability was reported in 'mm/ioremap.c' when performing a lookup of an non-existent page; a Denial of Service vulnerability was reported in the HFS and HFS+ (hfsplus) modules; and a remote Denial of Service vulnerability was reported due to a race condition in 'ebtables.c' when running on an SMP system that is operating under a heavy load. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for these vulnerabilities.	CAN-2005-3053 CAN-2005-3106 CAN-2005-3107 CAN-2005-3108 CAN-2005-3109 CAN-2005-3110		
Multiple Vendors Linux kernel 2.6-2.6.12 .1	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to an error when handling key rings; and a Denial of Service vulnerability was reported in the 'KE YCTL_JOIN_SESSION _KEYRING' operation due to an error when attempting to join a key management session. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.13-rc6-git 1.bz2 Ubuntu: : http://security.ubuntu.com/ubuntu/pool/main/l/ Trustix: http://http.trustix.org/pub/trustix/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-514.html** There is no exploit code required.	Linux Kernel Management Denials of Service CAN-2005-2098 CAN-2005-2099	Low	Secunia Advisory: SA16355, August 9, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 **RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005**
Multiple Vendors Novell Evolution 2.0.2-2.0.4; LibTIFF 3.6.1; sy Software Products CUPS 1.1.12-1.1.23, 1.1.10, 1.1.7, 1.1.6, 1.1.4 -5, 1.1.4-3, 1.1.4 -2, 1.1.4, 1.1.1, 1.0.4 -8, 1.0.4; Ubuntu 4.10, 5.04	A remote Denial of Service vulnerability has been reported due to insufficient validation of specific header values. Libtiff: http://freshmeat.net/redir/libtiff/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tiff/	LibTiff Tiff Image Header Remote Denial of Service CAN-2005-2452	Low	Security Focus Bugtraq ID 14417, July 29, 2005 Ubuntu Security Notice, USN-156-1, July 29, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:142, August 18, 2005 Turbolinux Security Advisory, TLSA-2005-89,

	Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** A Proof of Concept exploit has been published.			September 5, 2005 **Conectiva Linux Announcement, CLSA-2005:1021, October 6, 2005**
Multiple Vendors RedHat Enterprise Linux WS 4, WS 3, 2.1, IA64, ES 4, ES 3, 2.1, IA64, AS 4, AS 3, AS 2.1, IA64, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1, IA64; OpenSSL Project OpenSSL 0.9.3-0.9.8, 0.9.2 b, 0.9.1 c; FreeBSD 6.0 -STABLE, -RELEASE, 5.4 -RELENG, -RELEASE, 5.3 -STABLE, -RELENG, -RELEASE, 5.3, 5.2.1 -RELEASE, -RELENG, 5.2 -RELEASE, 5.2, 5.1 -RELENG, -RELEASE/Alpha, 5.1 -RELEASE-p5, -RELEASE, 5.1, 5.0 -RELENG, 5.0, 4.11 -STABLE, -RELENG, 4.10 -RELENG, -RELEASE, 4.10	A vulnerability has been reported due to the implementation of the 'SSL_OP_MSIE_SSLV2_RSA_PADDING' option that maintains compatibility with third party software, which could let a remote malicious user bypass security. OpenSSL: http://www.openssl.org/source/openssl-0.9.7h.tar.gz FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:21/openssl.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-800.html Gentoo: http://security.gentoo.org/glsa/glsa-200510-11.xml Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors OpenSSL Insecure Protocol Negotiation CAN-2005-2969	Medium	OpenSSL Security Advisory, October 11, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:21, October 11, 2005 RedHat Security Advisory, RHSA-2005:800-8, October 11, 2005 Gentoo Linux Security Advisory, GLSA 200510-11, October 12, 2005
Multiple Vendors Turbolinux Server 10.0, 8.0, Desktop 10.0, Turbolinux Home Appliance Server 1.0 Workgroup Edition, Hosting Edition; Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0; Sun Solaris 10.0 _x86, 10.0, 9.0 _x86 Update 2, 9.0 _x86, 9.0, Sun SEAM 1.0-1.0.2; SuSE Linux Professional 9.3 x86_64, 9.3, Linux Personal 9.3 x86_64, 9.3; RedHat Fedora Core3 & 4, Advanced Workstation for the Itanium Processor 2.1; MIT Kerberos 5 5.0 -1.4.1 & prior; Gentoo Linux	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability was reported when a malicious user submits a specially crafted TCP connection that causes the Key Distribution Center (KDC) to attempt to free random memory; a buffer overflow vulnerability was reported in KDC due to a boundary error when a specially crafted TCP or UDP request is submitted, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in 'krb/recvauth.c' which could let a remote malicious user execute arbitrary code. MIT: http://web.mit.edu/kerberos/advisories/2005-002-patch_1.4.1.txt.asc Mandriva: http://www.mandriva.com/security/advisories	Kerberos V5 Multiple Vulnerabilities CAN-2005-1174 CAN-2005-1175 CAN-2005-1689	High	MIT krb5 Security Advisory, 2005-002, July 12, 2005 RedHat Security Advisory, RHSA-2005:567-08, July 12, 2005 Sun(sm) Alert Notification, 101809, July 12, 2005 Fedora Update Notifications, FEDORA-2005-552 & 553, July 12, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Turbolinux Security Advisory TLSA-2005-78, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:

Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-567.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101809-1 SuSE: http://www.novell.com/linux/security/advisories.html Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://www.sgi.com/support/security/ Debian: http://www.debian.org/security/2005/dsa-757 Conectiva: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000993 Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101810-1 **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-562.html** Currently we are not aware of any exploits for these vulnerabilities.		119, July 14, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July, 14, 2005 SGI Security Advisory, 20050703-01-U, July 15, 2005 Debian Security Advisory, DSA-757-1, July 17, 2005 US-CERT VU#885830 US-CERT VU#623332 US-CERT VU#259798 Conectiva Linux Advisory, CLSA-2005:993, August 8, 2005 Sun(sm) Alert Notification Sun Alert ID: 101810, August 29, 2005 **RedHat Security Advisory, RHSA-2005:562-15, Updated October 5, 2005**

Multiple Vendors util-linux 2.8-2.13; Andries Brouwer util-linux 2.11 d, f, h, i, k, l, n, u, 2.10 s	A vulnerability has been reported because mounted filesystem options are improperly cleared due to a design flaw, which could let a remote malicious user obtain elevated privileges. Updates available at: http://www.kernel.org/pub/linux/utils/util-linux/testing/util-linux-2.12r-pre1.tar.gz Slackware: ftp://ftp.slackware.com/pub/slackware/ Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/u/util-linux/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-15.xml Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/u/util-linux/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** **Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101960-1** There is no exploit code required.	Util-Linux UMount Remounting Filesystem Elevated Privileges CAN-2005-2876	Medium	Security Focus, Bugtraq ID: 14816, September 12, 2005 Slackware Security Advisory, SSA:2005-255-02, September 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Ubuntu Security Notice, USN-184-1, September 19, 2005 Gentoo Linux Security Advisory, GLSA 200509-15, September 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:167, September 20, 2005 Debian Security Advisory, DSA 823-1, September 29, 2005 SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005 **Conectiva Linux Announcement, CLSA-2005:1022, October 6, 2005** **Sun(sm) Alert Notification Sun Alert ID: 101960, October 10, 2005**
Multiple Vendors xine xine-lib 1.1.0, 1.0-1.0.2, 0.9.13; Ubuntu Linux 5.0 4 powerpc, i386, amd64, ppc, ia64, ia32; Gentoo Linux	A format string vulnerability has been reported in 'input_cdda.c' when writing CD metadata retrieved from a CDDB server to a cache file, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200510-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xine-lib/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Mandriva: http://www.mandriva.com/security/advisories	Multiple Vendors CDDB Client Format String CAN-2005-2967	High	Gentoo Linux Security Advisory, GLSA 200510-08, October 8, 200 Ubuntu Security Notice, USN-196-1, October 10, 2005 Slackware Security Advisory, SSA:2005-283-01, October 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:180, October 11, 2005 Debian Security Advisory, DSA 863-1, October 12, 2005

	Debian: http://security.debian.org/pool/updates/main/x/xine-lib/ An exploit script has been published.			
Net-SNMP Net-SNMP 5.2.1, 5.2, 5.1-5.1.2, 5.0.3 -5.0.9, 5.0.1	A remote Denial of Service vulnerability has been reported when handling stream-based protocols. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=12694&package_id =11571&release_id=338899 Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-720.html Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/net-snmp/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-395.html** Currently we are not aware of any exploits for this vulnerability.	Net-SNMP Protocol Denial of Service CAN-2005-2177	Low	Secunia Advisory: SA15930, July 6, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Fedora Update Notifications, FEDORA-2005 -561 & 562, July 13, 2005 RedHat Security Advisory, RHSA-2005:720-04, August 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:137, August 11, 2005 Ubuntu Security Notice, USN-190-1, September 29, 2005 **RedHat Security Advisory, RHSA-2005:395-18, October 5, 2005**
Net-snmp Net-snmp 5.x	A vulnerability has been reported in 'fixproc' due to a failure to securely create temporary files in world writeable locations, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code with ROOT privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200505-18.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: https://rhn.redhat.com/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-395.html** There is no exploit code required.	Net-SNMP Fixprox Insecure Temporary File Creation CAN-2005-1740	High	Gentoo Linux Security Advisory, GLSA 200505-18, May 23, 2005 Fedora Update Notifications, FEDORA-2005 -561 & 562, July 13, 2005 RedHat Security Advisory, RHSA-2005:373-23, September 28, 2005 **RedHat Security Advisory, RHSA-2005:395-18, October 5, 2005**

OpenVMPS OpenVMPS 1.3	A format string vulnerability has been reported in the 'vmps_log()' function when logging various information using 'syslog(),' which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	OpenVMPS Logging Function Format String	High	Securiteam, October 12, 2005
Paul Vixie Vixie Cron 4.1	A vulnerability has been reported due to insecure creation of temporary files when crontab is executed with the '-e' option, which could let a malicious user obtain sensitive information. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-361.html** There is no exploit code required; however, a Proof of Concept exploit script has been published.	Vixie Cron Crontab Information Disclosure CAN-2005-1038	Medium	Security Focus, 13024, April 6, 2005 Fedora Update Notification, FEDORA-2005-320, April 15, 2005 Fedora Update Notifications, FEDORA-2005-550 & 551, July 12, 2005 **RedHat Security Advisory, RHSA-2005:361-19, October 5, 2005**
phpMyAdmin phpMyAdmin 2.6.4 -pl1	A vulnerability has been reported in 'libraries/grab_globals.lib.php' due to insufficient verification of the 'subform' array parameter before including files, which could let a malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPMyAdmin File Include	Medium	Secunia Advisory: SA17137, October 11, 2005
SGI IRIX 6.5.22 m	An input validation vulnerability has been reported in 'runpriv' when the user supplied command line is used to run authorized commands, which could let a malicious user execute arbitrary code with root privileges. Patch available at: http://support.sgi.com/ There is no exploit code required; however, a Proof of Concept exploit has been published.	SGI IRIX 'runpriv' Input Validation CAN-2005-2925	High	Security Tracker Alert ID: 1015031, October 10, 2005

Shorewall Shorewall 2.0.x, 2.2.x, 2.4.x	A vulnerability has been reported due to a failure to properly implement expected firewall rules for MAC address-based filtering, which could let a remote malicious user bypass firewall rules. Hotfixes available at: http://www.shorewall.net/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200507-20.xml **Debian: http://security.debian.org/pool/updates/main/s/shorewall/** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/shorewall/** There is no exploit code required.	Shorewall MACLIST Firewall Rules Bypass CAN-2005-2317	Medium	Secunia Advisory: SA16087, July 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:123, July 21, 2005 Gentoo Linux Security Advisory [ERRATA UPDATE], GLSA 200507-20:02, September 17, 2005 **Debian Security Advisory, DSA 849-1, October 8, 2005** **Ubuntu Security Notice, USN-197-1, October 10, 2005**
slocate slocate 2.7	A Denial of Service vulnerability has been reported when a specially crafted directory structure that contains long paths is submitted. Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: https://rhn.redhat.com/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-346.html** There is no exploit code required.	slocate Long Path Denial of Service CAN-2005-2499	Low	Mandriva Linux Security Update Advisory, MDKSA-2005:147, August 22, 2005 Turbolinux Security Advisory, TLSA-2005-91, September 20, 2005 RedHat Security Advisory, RHSA-2005:345-24, September 28, 2005 **RedHat Security Advisory, RHSA-2005:346-19, October 5, 2005**
Sun Microsystems, Inc. ONE Directory Server 5.2 patch 3, 5.2	A vulnerability has been reported in the HTTP admin interface due to an unspecified error, which could let a remote malicious user execute arbitrary code. Patches available at: http://sunsolve.sun.com/search/document.do?assetkey=1-21-117665-03-1 Currently we are not aware of any exploits for this vulnerability.	Sun Directory Server Remote Arbitrary Code Execution	High	NGSSoftware Insight Security Research Advisory, October 6, 2005
SuSE Linux Professional 10.0 OSS, 10.0 , Linux Personal 10.0 OSS, beagle 10.0	A Denial of Service vulnerability has been reported in the PowerSave daemon due to a flaw in the installed permissions. SUSE: ftp://ftp.suse.com/	SUSE Linux PowerSave Daemon Denial of Service	Low	SUSE Security Summary Report, SUSE-SR:2005:022, October 7, 2005

	pub/suse/i386/update/ There is no exploit code required.			
SuSE Linux Professional 9.3 x86_64, 9.3, Linux Personal 9.3 x86_64, 9.3	A buffer overflow vulnerability has been reported in Yast, which could let a malicious user execute arbitrary code with superuser privileges. **SUSE: ftp://ftp.SUSE.com/pub/SUSE** A Proof of Concept exploit has been published.	SuSE YaST Buffer Overflow CAN-2005-3013	High	Security Focus, Bugtraq ID: 14861, September 16, 2005 **SUSE Security Summary Report, SUSE-SR:2005:022, October 7, 2005**
SuSE SuSE Linux Standard Server 8.0, Linux School Server for i386, LINUX Retail Solution 8.0, SuSE Linux Openexchange Server 4.0, Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 10.0 OSS, 10.0, 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64, 8.2, Linux Personal 10.0 OSS, 10.0, 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64, 8.2, Linux Enterprise Server 9, 8, Linux Desktop 1.0	A vulnerability has been reported due to insecure permissions, which could let a malicious user overwrite package meta files. SUSE: ftp://ftp.SUSE.com/pub/SUSE There is no exploit code required.	SuSE YaST Package Repositories Insecure Permissions	Medium	SUSE Security Summary Report, SUSE-SR:2005:022, October 7, 2005
SuSE tomboy 10.0, 9.3; liferea 10.0, 9.3; blam 10.0, 9.3; beagle 10.0, 9.3; banshee 10.0	A vulnerability has been reported in the 'LD_LIBRARY_PATH' variable because it is handled in an unsafe manner by affected binaries, which could let a malicious user obtain elevated privileges. SUSE: ftp://ftp.suse.com/pub/suse/i386/update/ Currently we are not aware of any exploits for this vulnerability.	SUSE Linux Elevated Privileges CAN-2005-2966	Medium	SUSE Security Summary Report, SUSE-SR:2005:022, October 7, 2005
SuSE resmgr	Multiple vulnerabilities have been reported which could permit unauthorized access to USB devices. SUSE: ftp://ftp.SUSE.com/pub/SUSE Currently we are not aware of any exploits for these vulnerabilities.	SUSE ResMgr Unauthorized USB Device Access	Medium	SUSE Security Summary Report, SUSE-SR:2005:022, October 7, 2005
University of Washington UW-imapd imap-2004c1	A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version imap-2004g: ftp://ftp.cac.washington.edu/imap/ **Debian: http://security.debian.org/pool/updates/main/u/uw-imap/**	UW-imapd Denial of Service and Arbitrary Code Execution CAN-2005-2933	High	Secunia, Advisory: SA17062, October 5, 2005 **Debian Security Advisory, DSA 861-1, October 11, 2005** **Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005**

	Gentoo: **http://security.gentoo.org/glsa/glsa-200510-10.xml** Currently we are not aware of any exploits for this vulnerability.			
up-imapproxy up-imapproxy 1.2.4, 1.2.3	A format string vulnerability has been reported in the 'ParseBannerAndCapability()' function when processing the banner or capability line received from the IMAP server, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/u/up-imapproxy/ Currently we are not aware of any exploits for this vulnerability.	up-imapproxy Format String CAN-2005-2661	High	Debian Security Advisory DSA 852-1, October 9, 2005
Webmin Webmin 1.220, 1.210, 1.200; Usermin 1.150, 1.140, 1.130	A vulnerability has been reported in 'miniserv.pl' due to an input validation error in the authentication process, which could let a remote malicious user bypass certain security restrictions. Webmin: http://prdownloads.sourceforge.net/webadmin/webmin-1.230.tar.gz Usermin: http://prdownloads.sourceforge.net/webadmin/usermin-1.160.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200509-17.xml **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	Webmin / Usermin Remote PAM Authentication Bypass CAN-2005-3042	Medium	SNS Advisory No.83, September 20, 2005 Gentoo Linux Security Advisory, GLSA 200509-17, September 24, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:176, October 7, 2005**
Weex Weex 2.6.1 .5, 2.6.1	A format string vulnerability has been reported in the 'Log_Flush()' function when flushing an error log entry that contains format string specifiers, which could let a remote malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-09.xml** **Debian:** **http://security.debian.org/pool/updates/main/w/weex/** Currently we are not aware of any exploits for this vulnerability.	Weex Format String CAN-2005-3150	High	Secunia Advisory: SA17028, October 3, 2005 **Gentoo Linux Security Advisory, GLSA 200510-09, October 8, 2005** **Debian Security Advisory, DSA 855-1, October 10, 2005**

xloadimage xloadimage 4.1	A buffer overflow vulnerability has been reported when handling the title of a NIFF image when performing zoom, reduce, or rotate functions, which could let a remote malicious user execute arbitrary code. Debian: http://security.debian.org/pool/updates/main/x/xloadimage/ http://security.debian.org/pool/updates/main/x/xli/ Currently we are not aware of any exploits for this vulnerability.	Xloadimage NIFF Image Buffer Overflow CAN-2005-3178	High	Debian Security Advisories, DSA 858-1 & 859-1, October 10, 2005
Yukihiro Matsumoto Ruby 1.6 - 1.6.8, 1.8 - 1.8.2	A vulnerability has been reported in 'eval.c' due to a flaw in the logic that implements the SAFE level checks, which could let a remote malicious user bypass access restrictions to execute scripting code. Patches available at: ftp://ftp.ruby-lang.org/pub/ruby/1.6/1.6.8-patch1.gz Updates available at: http://www.ruby-lang.org/patches/ruby-1.8.2-xmlrpc-ipimethods-fix.diff **Gentoo:** **http://security.gentoo.org/glsa/glsa-200510-05.xml** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/universe/r/ruby1.8/** **Debian:** **http://security.debian.org/pool/updates/main/r/** There is no exploit code required.	Ruby Safe Level Restrictions Bypass CAN-2005-2337	Medium	Security Tracker Alert ID: 1014948, September 21, 2005 US-CERT VU#160012 **Gentoo Linux Security Advisory, GLSA 200510-05, October 6, 2005** **Ubuntu Security Notice, USN-195-1, October 10, 2005** **Debian Security Advisories, DSA 860-1 & DSA 862-1, October 11, 2005**
Zeroblog Zeroblog 1.2 a, 1.1 f	A Cross-Site Scripting vulnerability has been reported in 'thread.php' due to insufficient sanitization of the 'threadID' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Zeroblog Cross-Site Scripting	Medium	Security Focus Bugtraq ID: 15078, October 11, 2005
Zope Zope 2.6-2.8.1	A vulnerability has been reported in 'docutils' due to an unspecified error and affects all instances which exposes 'RestructuredText' functionality via the web. The impact was not specified. Hotfix available at: http://www.zope.org/Products/Zope/Hotfix_2005-10-09/security_	Zope 'Restructured Text' Unspecified Security Vulnerability	Not Specified	Zope Security Alert, October 12, 2005

	alert/Hot fix_2005-10-09.tar.gz Currently we are not aware of any exploits for this vulnerability.			

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attack Scripts	Common Name / CVE Reference	Risk	Source
Accelerated Enterprise Solutions Accelerated E Solutions	An SQL injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Accelerated E Solutions SQL Injection	Medium	Security Focus, Bugtraq ID: 15077, October 11, 2005
Andrea Bugada PHP Advanced Transfer Manager 1.30	A Cross-Site Scripting vulnerability has been reported because HTML documents can be uploaded to a location inside the web root, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Advanced Transfer Cross-Site Scripting	Medium	Security Tracker Alert ID: 1015021, October 10, 2005
BEA Systems Inc. WebLogic Express 6.x, 7.x, 8.x, 9.x, WebLogic Server 6.x, 7.x, 8.x, 9.x	BEA has released 24 advisories identifying various vulnerabilities affecting BEA WebLogic Server and WebLogic Express, which could let a local/remote malicious user facilitate attacks affecting the integrity, confidentiality, and availability of vulnerable computers. A vulnerability was reported due to an error in the thread handling of the server; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified input before returning to the user; a vulnerability was reported because Java client applications using the SSL protocol without specifying a user, may in certain situations be communicating insecurely with an unencrypted protocol; a vulnerability was reported when a Java client application creates both an insecure and secure connection to a server; a vulnerability was reported due to an error when deploying Web applications and EJBs; a vulnerability was reported because audit events may be posted with incorrect severity levels that have auditing enabled; a vulnerability was reported because IP addresses of machines behind a firewall can be disclosed via NAT (Network Address Translation); a vulnerability was reported in the 'nodemanager.config' file because the passphrase for the trust keystore is stored in clear text; a vulnerability was reported because Principals from a derived Principal class are not properly validated in certain situations; a vulnerability was reported because the servlet root URL pattern is not properly protecting servlets; a vulnerability was reported when restricting an unspecified internal servlet in the Administration server; a vulnerability was reported when importing security policies from other operating systems; a vulnerability was reported because the passphrase for the private key used to configure SSL is displayed in clear text on the terminal and stored in clear text in the server log file when creating a WebLogic server domain via the configuration wizard; a vulnerability was reported because certain servlet resources may not be properly protected after an error occurs during deployment when the 'fullyDelegateAuthorization' mode is enabled; a vulnerability was reported because system properties which may contain sensitive information are logged to the server log file; a vulnerability was reported because the password used to boot the server is stored in clear text in the Windows registry; a vulnerability was reported because a password that is included in a subject when using the IIOP (Internet Inter-ORB Protocol) protocol may be exposed in an exception to a remote client or in the server log; a vulnerability was reported because the lockout mechanism can be exploited to lockout the administrator via multiple incorrect login requests; a vulnerability was reported because a Deployer can use the weblogic.Deployer command using the insecure t3 protocol in communication with the Administration server; a vulnerability was reported because Multicast messages are sent in clear text in clusters; a vulnerability was reported when handling incorrect log records; a vulnerability was reported when handling malformed HTTP requests; a vulnerability was reported when handling servlets doing relative forwarding; and a vulnerability was reported in the userlockout security mechanism because more login requests than intended can be performed. Update information available at:	BEA WebLogic Server & WebLogic Express Multiple Vulnerabilities	Medium	Security Advisories, BEA05-80.02, BEA05-85 - BEA05-107, October 10, 2005

http://dev2dev.bea.com/advisoriesnotifications/

Some of these vulnerabilities do not require exploit code.

Ethereal Ethereal V0.10.11	Multiple dissector and zlib vulnerabilities have been reported in Ethereal that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version 0.10.12: http://www.ethereal.com/download.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-687.html SUSE: ftp://ftp.suse.com/pub/suse/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-185.pdf SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Debian: http://security.debian.org/pool/updates/main/e/ethereal/** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Denial of Service or Arbitrary Code Execution CAN-2005-2361 CAN-2005-2362 CAN-2005-2363 CAN-2005-2364 CAN-2005-2365 CAN-2005-2366 CAN-2005-2367	High	Secunia, Advisory: SA16225, July 27, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:131, August 4, 2005 RedHat Security Advisory, RHSA-2005:687-03, August 10, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 Avaya Security Advisory, ASA-2005-185, August 30, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 Conectiva Linux Announce-ment, CLSA-2005:1003, September 13, 2005 **Debian Security Advisory, DSA 853-1, October 9, 2005**
Hewlett Packard Company OpenView Event Correlation Services 3.31-3.33 Windows, 3.31-3.33 Solaris, 3.31-3.33 Linux, 3.31-3.33 HP-UX	A vulnerability has been reported in the 'cgi-bin/ecscmg.ovpl' script due to insufficient validation of user-supplied input before using as part of a system command, which could let a remote malicious user obtain elevated privileges. As a workaround, the vendor indicates that you can move the 'ecscmg.ovpl' file from the cgi-bin directory into another directory. The directory should not have write permissions for ordinary users. **Patches available at: http://support.openview.hp.com/patches/patch_index.jsp** Currently we are not aware of any exploits for this vulnerability.	HP OpenView Event Correlation Services Remote Elevated Privileges	Medium	HP Security Bulletin, HPSBMA01225, September 4, 2005 **HP Security Bulletin, HPSBMA01225, October 4, 2005**
IBM Tivoli Monitoring for Web Infrastructure 5.1.2, 5.1, 5.0	Multiple remote Denial of Service vulnerabilities have been reported when older versions of IBM HTTP server are installed with the WHC (Web Health Console). Update information available at: http://www-1.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg27005198 Currently we are not aware of any exploits for these vulnerabilities.	IBM Tivoli Monitoring Web Health Console Multiple Denial of Service	Low	Secunia Advisory: SA17065, October 5, 2005
Jean-Baptiste Lamy Py2Play 0.1.7	A vulnerability has been reported due to insufficient validation/ restriction of serialized Python objects (pickles) used when receiving objects over a peer-to-peer game network, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200509-09.xml **Debian:**	Py2Play Object Remote Python Code Execution CAN-2005-2875	High	Gentoo Linux Security Advisory GLSA 200509-09, September 17, 2005 **Debian Security Advisory, DSA 856-1, October 10, 2005**

	http://security.debian.org/pool/updates/main/p/py2play/ There is no exploit code required.			
MediaWiki MediaWiki 1.4.10	A vulnerability has been reported because mediawiki Wiki edit submission handling could cause corruption of the previous revision in the database if an abnormal URL was used. SUSE: ftp://ftp.SUSE.com/pub/SUSE There is no exploit code required.	MediaWiki Database Corruption CAN-2005-3166	Medium	SUSE Security Summary Report, SUSE-SR:2005:022, October 7, 2005
MediaWiki MediaWiki 1.5 alpha1&2, bet1-beta3, 1.4-1.4.10, 1.3.13, 1.3-1.3.11	A Cross-Site Scripting vulnerability has been reported in inline style attributes due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/wikipedia/mediawiki-1.4.11.tar.gz There is no exploit code required.	MediaWiki HTML Inline Style Attributes Cross-Site Scripting CAN-2005-3167	Medium	Security Focus, Bugtraq ID: 15024, October 6, 2005
Moritz Naumann SquirrelMail Address Add Plugin 2.0, 1.9	A Cross-Site Scripting vulnerability has been reported in 'add.php' due to insufficient sanitization of the 'first' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://squirrelmail.org/plugin_download.php?id=101&rev=1210 **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required; however, a Proof of Concept exploit has been published.	SquirrelMail Cross-Site Scripting CAN-2005-3128	Medium	Security Tracker Alert ID: 1014988, September 29, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:178, October 11, 2005**
Mozilla Firefox 1.0.6; Mozilla Browser 1.7.11, 1.7-1.7.9; Thunderbird 1.0-1.0.6	A vulnerability has been reported which could let a remote malicious user execute arbitrary commands via shell metacharacters in a URL. Upgrades available at: http://www.mozilla.org/products/firefox/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-785.html http://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.479350 SGI: ftp://patches.sgi.com/	Mozilla Browser/Firefox Arbitrary Command Execution CAN-2005-2968	High	Security Focus Bugtraq ID: 14888, September 21, 2005 Security Focus Bugtraq ID: 14888, September 22, 2005 RedHat Security Advisories, RHSA-2005:785-9 & 789-11, September 22, 2005 Ubuntu Security Notices, USN-USN-186-1 & 186-2, September 23 & 25, 2005 US-CERT VU#914681 Mandriva Linux Security Update Advisory, MDKSA-2005:169, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 SGI Security Advisory, 20050903-02-U, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1017,

	support/free/security/advisories/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Slackware: ftp://ftp.slackware.com/pub/slackware/** **Mandriva: http://www.mandriva.com/security/advisories** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/** There is no exploit code required; however, a Proof of Concept exploit has been published.			September 28, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 **Slackware Security Advisory, SSA:2005-278-01, October 5, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005** **Ubuntu Security Notice, USN-200-1, October 11, 2005**
Mozilla.org Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported due to a failure in the application to properly verify Document Object Model (DOM) property values, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-434.html http://rhn.redhat.com/errata/RHSA-2005-435.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ SUSE: ftp://ftp.suse.com/pub/suse/ SGI: ftp://patches.sgi.com/support/ free/security/advisories/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.	Mozilla Suite And Firefox DOM Property Overrides CAN-2005-1532	High	Mozilla Foundation Security Advisory, 2005-44, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 Ubuntu Security Notice, USN-134-1, May 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 SGI Security Advisory, 20050503-01-U, June 8, 2005 SUSE Security Announcement, SUSE-SA:2005:030, June 9, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 HP Security Bulletin, HPSBUX01133, August 8, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 **Ubuntu Security Notice, USN-155-3, October 04, 2005**

com/ubuntu/pool/
main/m/mozilla-
thunderbird/

HP:
http://h20000.www2.hp.
com/bizsupport/
TechSupport/
Document.jsp?objectID=
PSD_HPSBUX01133

Debian:
http://security.debian.org/
pool/updates/main/m/
mozilla-thunderbird/

Ubuntu:
http://security.ubuntu.
com/ubuntu/pool/
main/m/

Currently we are not aware of any exploits for this vulnerability.

Mozilla.org Netscape 8.0.3.3, 7.2; Mozilla Firefox 1.5 Beta1, 1.0.6; Mozilla Browser 1.7.11; Mozilla Thunderbird 1.0.6	A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code. Patches available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-769.html http://rhn.redhat.com/errata/RHSA-2005-768.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **HP:** **http://software.hp.com/** **Mandriva:** **http://www.mandriva.com/security/advisories** A Proof of Concept exploit script has been published.	Mozilla/Netscape/ Firefox Browsers Domain Name Buffer Overflow CAN-2005-2871	High	Security Focus, Bugtraq ID: 14784, September 10, 2005 RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9, 2005 Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005 Ubuntu Security Notice, USN-181-1, September 12, 2005 US-CERT VU#573857 Gentoo Linux Security Advisory GLSA 200509-11, September 18, 2005 Security Focus, Bugtraq ID: 14784, September 22, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200509-11:02, September 29, 2005 Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Debian Security Advisory, DSA 837-1, October 2, 2005 Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 **HP Security Bulletin, HPSBUX01231, October 3, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005**

Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported when processing 'javascript:' URLs, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-434.html http://rhn.redhat.com/errata/RHSA-2005-435.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/** Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox Wrapped 'javascript:' URLs CAN-2005-1531	High	Mozilla Foundation Security Advisory, 2005-43, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 Ubuntu Security Notice, USN-134-1, May 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 SGI Security Advisory, 20050503-01-U, June 8, 2005 SUSE Security Announcement, SUSE-SA:2005:030, June 9, 2005 **Ubuntu Security Notice, USN-155-3, October 04, 2005**
Multiple Vendors Mozilla Firefox 1.0-1.0.6; Mozilla Browser 1.7-1.7.11	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when processing malformed XBM images, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when unicode sequences contain 'zero-width non-joiner' characters, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported due to a flaw when making XMLHttp requests, which could let a remote malicious user spoof XMLHttpRequest headers; a vulnerability was reported because a remote malicious user can create specially crafted HTML that spoofs XML objects to create an XBL binding to execute arbitrary JavaScript with elevated (chrome) permissions; an integer overflow vulnerability was reported in the JavaScript engine, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a remote malicious user can load privileged 'chrome' pages from an unprivileged 'about:' page, which could lead to unauthorized access; and a window spoofing vulnerability was reported when a blank 'chrom' canvas is obtained by opening a window from a reference to a closed window, which could let a remote malicious user conduct phishing type attacks. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ RedHat: https://rhn.redhat.com/errata/RHSA-2005-789.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/ Mandriva: http://www.mandriva.com/security/	Mozilla Browser / Firefox Multiple Vulnerabilities CAN-2005-2701 CAN-2005-2702 CAN-2005-2703 CAN-2005-2704 CAN-2005-2705 CAN-2005-2706 CAN-2005-2707	High	Mozilla Foundation Security Advisory, 2005-58, September 22, 2005 RedHat Security Advisory, RHSA-2005:789-11, September 22, 2005 Ubuntu Security Notices, USN-186-1 & 186-2, September 23 & 25, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:169 & 170, September 26, 2005 Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005 Slackware Security Advisory, SSA:2005-269-01, September 26, 2005 SGI Security Advisory, 20050903-02-U, September 28, 2005 Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005 Gentoo Linux Security Advisory [UPDATE] , September 29, 2005

	advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.479350 SGI: ftp://patches.sgi.com/support/free/security/advisories/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/glsa/glsa-200509-11.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Mandriva:** **http://www.mandriva.com/security/advisories** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/** Currently we are not aware of any exploits for these vulnerabilities.			SUSE Security Announcement, SUSE-SA:2005:058, September 30, 2005 Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005 Debian Security Advisory, DSA 838-1, October 2, 2005 Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005** **Ubuntu Security Notice, USN-200-1, October 11, 2005**
Multiple Vendors Windows XP, Server 2003 Windows Services for UNIX 2.2, 3.0, 3.5 when running on Windows 2000 Berbers V5 Release 1.3.6 AAA Intuit LX, Converged Communications Server (CCS) 2.x, MN100, Modular Messaging 2.x, S8XXX Media Servers	An information disclosure vulnerability has been reported that could let a remote malicious user read the session variables for users who have open connections to a malicious telnet server. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-033.mspx RedHat: ftp://updates.redhat.com/enterprise Microsoft: http://www.microsoft.com/technet/security/Bulletin/MS05-033.mspx SUSE: ftp://ftp.SUSE.com/pub/SUSE AAA: http://support.avaya.com/elmodocs2/security/ASA-2005-145	Multiple Vendor Telnet Client Information Disclosure CAN-2005-1205 CAN-2005-0488	Medium	Microsoft, MS05-033, June 14, 2004 US-CERT VU#800829 iD EFENSE Security Advisory, June 14, 2005 Red Hat Security Advisory, RHSA-2005:504-00, June 14, 2005 Microsoft Security Bulletin, MS05-033 & V1.1, June 14 & 15, 2005 SUSE Security Summary Report, SUSE-SR:2005:016, June 17, 2005 AAA Security Advisory,

	RHSA-2005-504.pdf Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-567.html SGI: ftp://oss.sgi.com/projects/sgipropack/download/3/updates/ Mandriva: http://www.mandriva.com/security/advisories Microsoft: Bulletin revised to communicate the availability of security updates for Services for UNIX 2.0 and Services for UNIX 2.1. The "Security Update Information" section has also be revised with updated information related to the additional security updates. F5: http://tech.f5.com/home/bigip/solutions/advisories/ sol4616.html SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.35 **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-562.html** Currently we are not aware of any exploits for this vulnerability.			ASA-2005-145, June 17, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 RedHat Security Advisory, RHSA-2005:567-08, July 12, 2005 SGI Security Advisories, 20050605-01-U, 20050702-01-U, & 20050703-01-U, July 12 & 15, 2005 Microsoft Security Bulletin, MS05-033 V2.0 July 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:119, July 14, 2005 SCO Security Advisory, SCOSA-2005.35, September 1, 2005 **RedHat Security Advisory, RHSA-2005:562-15, Updated October 5, 2005**
Multiple Vendors complete list available at: http://www.securityfocus.com/bid/15046	A vulnerability has been reported in multiple antivirus products when processing a specially altered archive file that contains a fake, misleading MS-DOS executable MZ header, which could let malformed archive files bypass detection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Multiple Vendor Antivirus Products Malformed Archives Scan Bypass	Medium	Security Focus, Bugtraq ID: 15046, October 8, 2005
Multiple Vendors PHPXMLRPC 1.1.1; PEAR XML_RPC 1.3.3; Drupal 4.6-4.6.2, 4.5- 4.5.4; Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.; MailWatch for MailScanner 1.0.1; eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0	A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. PHPXMLRPC : http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc.1.2.tgz?download Pear: http://pear.php.net/get/XML_RPC-1.4.0.tgz Drupal: http://drupal.org/files/projects/drupal-4.5.5.tar.gz eGroupWare: http://prdownloads.sourceforge.net/egroupware/eGroupWare-1.0.0.009.tar .gz?download MailWatch: http://prdownloads.sourceforge.net/mailwatch/mailwatch-1.0.2.tar.gz Nucleus:	PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution CAN-2005-2498	High	Security Focus, Bugtraq ID 14560, August 15, 2995 Security Focus, Bugtraq ID 14560, August 18, 2995 RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005 Ubuntu Security Notice, USN-171-1, August 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:146, August 22, 2005 Gentoo Linux Security Advisory, GLSA 200508-13 & 14, & 200508-18, August 24 & 26, 2005 Fedora Update Notifications, FEDORA-2005-809 & 810, August 25, 2005 Debian Security Advisory, DSA 789-1, August 29,

http://prdownloads.sourceforge.net/nucleuscms/nucleus-xmlrpc-patch.zip ?download

RedHat:
http://rhn.redhat.com/errata/RHSA-2005-748.html

Ubuntu:
http://security.ubuntu.com/ubuntu/pool/main/p/php4/

Mandriva:
http://www.mandriva.com/security/advisories

Gentoo:
http://security.gentoo.org/glsa/glsa-200508-13.xml

http://security.gentoo.org/glsa/glsa-200508-14.xml

http://security.gentoo.org/glsa/glsa-200508-18.xml

Fedora:
http://download.fedora.redhat.com/pub/fedora/linux/core/updates/

Debian:
http://security.debian.org/pool/updates/main/p/php4/

SUSE:
ftp://ftp.suse.com/pub/suse/

Gentoo:
http://security.gentoo.org/glsa/glsa-200508-20.xml

http://security.gentoo.org/glsa/glsa-200508-21.xml

Slackware:
ftp://ftp.slackware.com/pub/slackware/

Debian:
http://security.debian.org/pool/updates/main/p/phpgroupware/

SGI:
ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/

Slackware:
ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/

ftp://ftp.slackware.com/pub/slackware/slackware-10.1/testing/packages/php-5.0.5/php-5.0.5-i486-1.tgz

Gentoo:

2005

SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005

Gentoo Linux Security Advisory, GLSA GLSA 200508-20& 200508-21, August 30 & 31, 2005

Slackware Security Advisory, SSA:2005-242-02, August 31, 2005

Debian Security Advisory, DSA 798-1, September 2, 2005

SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005

SGI Security Advisory, 20050901-01-U, September 7, 2005

Slackware Security Advisories, SSA:2005-251-03 & 251-04, September 9, 2005

Gentoo Linux Security Advisory, GLSA 200509-19, September 27, 2005

Debian Security Advisory, DSA 840-1, October 4, 2005

Debian Security Advisory, DSA 842-1, October 4, 2005

Conectiva Linux Announcement, CLSA-2005:1024, October 7, 2005

	http://security.gentoo.org/glsa/glsa-200509-19.xml Debian: http://security.debian.org/pool/updates/main/d/drupal/ **Debian:** **http://security.debian.org/pool/updates/main/e/egroupware/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.			
Multiple Vendors See US-CERT VU#222750 for complete list	Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) do not adequately validate ICMP error messages, which could let a remote malicious user cause a Denial of Service. Cisco: http://www.cisco.com/warp/ public/707/cisco-sa-20050412-icmp.shtml IBM: ftp://aix.software.ibm.com/aix/efixes/security/icmp efix.tar.Z RedHat: http://rhn.redhat.com/errata/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1 ALAXALA: Customers are advised to contact the vendor in regards to obtaining and applying the appropriate update. HP: www2.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU0116 HP: www2.itrc.hp.com/service/ cki/docDisplay.do?docId=HPSBTU01210 **HPSBTU01210 Rev 1: New ERP kits are available for HP Tru64 Unix V5.1B-3, V5.1B-2/PK4, and V5.1A PK6.** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service CAN-2004-1060 CAN-2004-0790 CAN-2004-0791	Low	US-CERT VU#222750 Sun(sm) Alert Notification, 57746, April 29, 2005 US-CERT VU#415294 Security Focus, 13124, May 21, 2005 HP Security Bulletin, HPSBTU01210, July 17, 2005 HP Security Bulletin, HPSBUX0116 Rev 4, July 19, 2005 **HP Security Bulletin, HPSBTU01210 Rev 1, October 4, 2005**
my Webland MyBloggie 2.1.3	An SQL injection vulnerability has been reported in the 'search.php' script due to insufficient validation of the user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MyBloggie SQL Injection	Medium	Security Focus, Bugtraq ID: 15017, October 6, 2005

MySQL AB MySQL 4.0 .0-4.0.11, 5.0 .0-5.0.4	A vulnerability has been reported in the 'mysql_install_db' script due to the insecure creation of temporary files, which could let a malicious user obtain unauthorized access. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ Debian: http://security.debian.org/pool/updates/main/m/mysql-dfsg-4.1/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-685.html** There is no exploit code required.	MySQL 'mysql_install_db' Insecure Temporary File Creation CAN-2005-1636	Medium	Security Focus, 13660, May 17, 2005 Fedora Update Notification, FEDORA-2005-557, July 20, 2005 Debian Security Advisory, DSA 783-1, August 24, 2005 **RedHat Security Advisory, RHSA-2005:685-5, October 5, 2005**
MySQL AB MySQL 5.0 .0-0-5.0.4, 4.1 .0-0-4.1.5, 4.0.24, 4.0.21, 4.0.20 , 4.0.18, 4.0 .0-4.0.15	A buffer overflow vulnerability has been reported due to insufficient bounds checking of data that is supplied as an argument in a user-defined function, which could let a remote malicious user execute arbitrary code. This issue is reportedly addressed in MySQL versions 4.0.25, 4.1.13, and 5.0.7-beta available at: http://dev.mysql.com/downloads/ Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg **Debian:** **http://security.debian.org/pool/updates/main/m/** SUSE: ftp://ftp.SUSE.com/pub/SUSE Debian: http://security.debian.org/pool/updates/main/m/mysql-dfsg-4.1/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	MySQL User-Defined Function Buffer Overflow CAN-2005-2558	High	Security Focus 14509 , August 8, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:163, September 12, 2005 Ubuntu Security Notice, USN-180-1, September 12, 2005 Debian Security Advisories, DSA 829-1 & 831-1, September 30, 2005 SUSE Security Summary Report, SUSE-SR:2005:021, September 30, 2005 Debian Security Advisory, DSA 833-1, October 1, 2005 **Conectiva Linux Announcement, CLSA-2005:1023, October 6, 2005**
Novell NetMail 3.52 C1, 3.52 A-C, 3.52	A buffer overflow vulnerability has been reported in the Network Messaging Application Protocol (NMAP) due to a boundary error when handling an overly long user name in the 'USER' command, which could let a remote malicious user execute arbitrary code. Updates available at: http://support.novell.com/servlet/filedownload/ Currently we are not aware of any exploits for this vulnerability.	Novell NetMail NMAP Agent Remote Buffer Overflow CAN-2005-2469	High	Novell Technical Information Documents, TID2972340, TID2972433, & TID2972438, October 10, 2005
OpenSSH OpenSSH 4.1, 4.0, p1	Several vulnerabilities have been reported: a vulnerability was reported due to an error when handling dynamic port forwarding when no listen address is specified, which could let a remote malicious user cause "GatewayPorts" to be incorrectly activated; and a vulnerability was reported due to an error when handling GSSAPI credential delegation, which could let a remote malicious user be delegated with GSSAPI credentials. Upgrades available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-4.2.tar.gz	OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials CAN-2005-2797 CAN-2005-2798	Medium	Secunia Advisory: SA16686, September 2, 2005 Fedora Update Notification, FEDORA-2005-858, September 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-527.html** **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.			Slackware Security Advisory, SSA:2005-251-03, September 9, 2005 Fedora Update Notification, FEDORA-2005-860, September 12, 2005 **RedHat Security Advisory, RHSA-2005:527-16, October 5, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:172, October 6, 2005**
OpenVPN OpenVPN 2.0 , 1.6 .0, 1.5 .0, 1.4.0-1.4.3, 1.3.2 , 1.2.1	Multiple remote Denial of Service vulnerabilities have been reported: a Denial of Service vulnerability was reported when flushing the OpenSSL error due to a failed client certificate authentication; a Denial of Service vulnerability was reported when flushing the OpenSSL error when a received packet fails to decrypt; a Denial of Service vulnerability was reported when configured in the 'dev tap' ethernet bridging mode; and a Denial of Service vulnerability was reported when two or more clients connect to the server at the same time using the same client certificate. Upgrades available at: http://openvpn.net/release/openvpn-2.0.1.tar.gz Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE **Debian:** **http://security.debian.org/pool/updates/main/o/openvpn/** There is no exploit code required.	OpenVPN Multiple Remote Denials of Service CAN-2005-2531 CAN-2005-2532 CAN-2005-2533 CAN-2005-2534	Low	Secunia Advisory: SA16463, August 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:145, August 22, 2005 SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005 **Debian Security Advisory, DSA 851-1, October 9, 2005**
OScommerce Additional Images 1.x (module for osCommerce	An SQL injection vulnerability has been reported in 'product_info.php' due to insufficient sanitization of the 'products_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	OScommerce SQL Injection	Medium	Secunia Advisory: SA17082, October 6, 2005
PHP-Fusion PHP-Fusion 6.0.109	SQL injection vulnerabilities have been reported in 'photogallery.php' due to insufficient sanitization of the 'album' and 'photo' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. **Upgrades available at:** **http://prdownloads.sourceforge.net/php-fusion/php-fusion-6.00.110.zip? download** There is no exploit code required.	PHP-Fusion Multiple SQL Injection CAN-2005-3160 CAN-2005-3162	Medium	Secunia Advisory: SA17048, October 4, 2005 **Security Focus, Bugtraq ID: 15005, October 6, 2005**

Planet Technology Corporation FGSW-2402RS 1.2 (firmware)	A vulnerability has been reported because a default password exits for resetting the password, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Planet Technology FGSW-2402RS Switch Backdoor Password	Medium	Security Focus, Bugtraq ID: 15014, October 6, 2005
Sun Microsystems Inc. Java System Application Server 7.0 UR6 Standard Edition, 7.0 UR6 Platform Edition, 7.0 UR5 Standard Edition, 7.0 UR5 Platform Edition, 7.0 UR4, 7.0 2004Q2 R2 Standard, 7.0 2004Q2 R2 Enterprise, 7.0 2004Q2 R1Standard, 7.0 2004Q2 R1Enterprise, 7.0 Standard Edition, 7.0 Platform Edition, Enterprise Edition, 7.0 2004Q2	A vulnerability has been reported due to an unspecified error in the Java Server Page, which could let a remote malicious user obtain sensitive information. Patch information available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101910-1 Currently we are not aware of any exploits for this vulnerability.	Sun Java System Application Server Java Server Page Information Disclosure	Medium	Sun(sm) Alert Notification Sun Alert ID: 101910, October 11, 2005
TellMe TellMe 1.2	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'q_IP' and 'q_Host parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'q_Host' parameter due to insufficient sanitization before using as a command line to 'whois,' which could let a remote malicious user obtain sensitive information. Upgrade available at: http://kimihia.org.nz/projects/tellme/files/tellme-1.3_php3.txt There is no exploit code required; however, a Proof of Concept exploit has been published.	TellMe Cross-Site Scripting & Information Disclosure	Medium	Secunia Advisory: SA17078, October 6, 2005
UtopiaSoft Utopia News Pro 1.1.3	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'header.php' due to insufficient sanitization of the 'sitetitle' parameter and in 'footer.php' due to insufficient sanitization of the 'version' and 'query_count' parameters, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'news.php' due to insufficient sanitization of the 'newsid' parameter before using in a SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Utopia News Pro Cross-Site Scripting & SQL Injection	Medium	Security Tracker Alert ID: 1015016, October 7, 2005
Veritas Software NetBackup Server 6.0, 5.1, 5.0, NetBackup Enterprise Server 6.0, 5.1, 5.0, NetBackup DataCenter 4.5 MP, 4.5 FP, NetBackup BusinessServer 4.5 MP, 4.5 FP	A format string vulnerability has been reported in the Java user-interface, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Patch information available at: http://seer.support.veritas.com/docs/279085.htm Currently we are not aware of any exploits for this vulnerability.	VERITAS NetBackup Java User-Interface Remote Format String CAN-2005-2715	High	Veritas Document ID: 279085, October 12, 2005 US-CERT VU#495556

versatile BulletinBoard versatile BulletinBoard 1.0 .0.RC2	Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of some input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported in 'imagewin.php' due to insufficient sanitization of the 'file' parameter and in 'dereferrer.php' due to insufficient sanitization of the 'url' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported when the 'getversions.php' script is accessed directly, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however an exploit script has been published.	versatile BulletinBoard Cross-Site Scripting, SQL Injection & Information Disclosure	Medium	Secunia Advisory: SA17174, October 12, 2005
W3C Libwww 5.4	Multiple unspecified vulnerabilities have been reported including a buffer overflow and vulnerabilities related to the handling of multipart/byteranges content. The impact was not specified. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Currently we are not aware of any exploits for these vulnerabilities.	W3C Libwww Multiple Unspecified Vulnerabilities CAN-2005-3183	Not Specified	Fedora Update Notifications, FEDORA- 2005-952 & 953, October 7, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Industry unites on next-gen Wi-Fi:** Some of the world's biggest IT companies have united behind the 802.11n standard for next-generation wireless broadband. The Enhanced Wireless Consortium (EWC) which includes Intel, Apple, Sony, and Cisco promote the standard. Source: http://www.vnunet.com/vnunet/news/2143664/industry-unites-generation-wi.
- **Competitors Catching Up With Symbian Smartphone Platform: Study:** According to a study released by ABI Research, the Symbian OS still is the world's dominant smartphone operating system, but Microsoft's Windows Mobile is gaining and Linux could catch on as well. The study doesn't predict market shares for each of the platforms but, discusses their strengths and weaknesses. Source: http://www.mobilepipeline.com/showArticle.jhtml?articleID=172300427**.**
- **Securing mobile data more important than viruses:** According to speakers at Symbian's Smartphone Show in London, enterprises with workers that can access corporate data from mobile devices should be less concerned about mobile viruses and more focused on setting and enforcing rules for securing the data. Very few real mobile viruses have actually proliferated in the market. Source: http://www.infoworld.com/article/05/10/12/HNsecuringmobiledata_1.html.
- **Attackers Could Text Message Cell Services To Death:** According to a group of academic researchers from Pennsylvania State University, cell phone networks are so vulnerable to denial-of-service-style attacks that an assault carried out by a mid-sized bot network could bring down the United States' entire mobile infrastructure. A paper that will be presented at the ACM Conference on Computer and Communications Security in November, outlines how an attack exploiting weaknesses in SMS (Short Message Service) could overload a cell network, and bring both voice and text messaging to a screeching stop. Source: http://www.techweb.com/showArticle.jhtml?articleID=171203666.
- **Wireless Applications Not Quite Ready For Prime Time:** At the Mobile Business Expo, the opening keynote speaker disproved that wireless applications are ready for large-scale deployments. Several things need to occur before this can happen. Carriers have to start focusing on business users more, and the industry has to move away from proprietary mobile applications, such as the ones Research In Motion offers for BlackBerry devices, and toward open standard applications that truly extend mobile applications beyond E-mail. Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=0OCJICEMD4WTWQSNDBECKH0CJUMEKJVN?articleID=171204530 .

Wireless Vulnerabilities

- Microsoft Windows XP Wireless Zero Configuration Service Information Disclosure: A vulnerability has been reported in Windows XP Wireless Zero Configuration Service that could let remote malicious users disclose information.
- Linux Kernel Denial of Service & Information Disclosure: A vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes when increasing the length, which could let a malicious user obtain sensitive information.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
October 12, 2005	caigw.c	No	Script that exploits the CA iGateway Debug Mode HTTP GET Request Buffer Overflow vulnerability.
October 12, 2005	MallocMaleficarum.txt	N/A	The Malloc Maleficarum discusses the next generation of possible glibc malloc exploitation techniques.
October 12, 2005	phpshopSQL.txt	Yes	Exploit details for the PhpShop SQL Injection vulnerability.

October 12, 2005	r57phpbb_admin2exec.pl.txt	No	Exploit for the Remote phpBB Command Execution vulnerability.
October 12, 2005	VAstacksmash.txt	N/A	A paper that presents an attack that works by exploiting static addresses in Linux.
October 11, 2005	versatile_xpl.php versatile100RC2_xpl.html	No	Exploits for the VersatileBulletinBoard Multiple SQL Injection vulnerabilities.
October 10, 2005	phpmyadmin_locfile.pl	No	Proof of Concept exploit for the PHPMyAdmin File Include vulnerability.
October 10, 2005	xine-cddb-server.pl	Yes	Script that exploits the Xine-Lib Remote CDDB Information Format String vulnerability.
October 8, 2005	aenovoSQL.txt	No	Detailed exploitation for the Aenovo SQL injection & Cross-Site Scripting vulnerabilities.
October 8, 2005	AVCraftedArchive.txt	No	Exploitation details for the Anti-Virus bypass archive vulnerability.
October 8, 2005	cyphor.php	No	Script that exploits the Cyphor Cross-Site Scripting and SQL Injection Vulnerabilities.
October 8, 2005	cyphor019.html	No	Proof of Concept exploit for the Cyphor Cross-Site Scripting & SQL Injection vulnerabilities.
October 8, 2005	phpCounter.txt	No	Exploitation details for the PHPCounter Cross-Site Scripting & SQL injection vulnerabilities.
October 8, 2005	smackthestack.txt	N/A	A whitepaper that discusses five creative methods used to overcome various stack protection patches. These methods are not limited to this patch, but provide a different approach to the buffer overflow exploiting scheme.
October 8, 2005	xine-cddb-server.pl.txt	Yes	Proof of Concept exploit for the Multiple Vendors CDDB Client Format String vulnerability.
October 7, 2005	mailenable.cpp	Yes	Exploit for the MailEnable Arbitrary Code Execution vulnerability.
October 7, 2005	utopia_xpl.php	No	Exploit for the Utopia News Pro SQL Injection vulnerability.
October 7, 2005	utopia113.html	No	Proof of Concept exploit for the Utopia News Pro Cross-Site Scripting & SQL Injection vulnerabilities.
October 7, 2005	xloadFlaws.tgz	Yes	Proof of Concept exploit for the Xloadimage Image Title Name Buffer Overflow vulnerabilities.
October 6, 2005	amap-5.2.tar.gz	N/A	A next-generation scanning tool that allows you to identify the applications that are running on a specific port by connecting to the port(s) and sending trigger packets.
October 6, 2005	caigw-win32.c	No	Exploit for the Computer Associates Multiple Product HTTP Request Remote Unspecified Buffer Overflow vulnerability.
October 6, 2005	hydra-5.0-src.tar.gz	N/A	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more.
October 6, 2005	no-nx.pdf	N/A	A whitepaper that analyzes NX technology weaknesses and contains sample code for the Hammer/Linux platform.
October 6, 2005	THC-Scan-2.01.zip	N/A	A wardialer that works under DOS, Win95/98/NT/2K/XP, and all DOS emulators (UNiX) on all 80x86 processors.

[back to top]

Trends

- **Survey: IT spending to rise in 2006:** In survey results released by Gartner, U.S. companies plan to hike their spending on technology by 5.5 percent in 2006. The increased technology investments will be spent on application development and integration. Spending on security and storage segments will level off in 2006, and mobile devices will become a major purchasing priority. In addition, development tools and middleware will also attract investment. Source: http://news.com.com/Survey+IT+spending+to+rise+in+2006/2100-7342_3-5893853.html?tag=nefd.top .
- **Spyware threat escalating, expert warns:** According to security experts spyware is becoming increasingly more sophisticated. Users are failing to take basic steps to protect themselves against this threat. This is a problem that should scare big businesses as they face up to the fact that important data could be leaking out of their organizations daily. Source: http://news.com.com/Spyware+threat+escalating%2C+expert+warns/2100-1029_3-5893267.html?tag=cd.top.
- **Malicious attack trends: good, bad, and worse:** According to Symantec's Internet Security Threat Report, Vol. VII, automated code and for-profit hackers have information theft on the rise. Even though the Symantec report represents just one vendor's view on the changing threat space, Symantec is pulling its data from 24,000 sensors in more than 180 companies participating in its DeepSight Threat Management System and Symantec Managed Security Services.
  Source: http://www.infoworld.com/article/05/10/07/41OPsecadvise_1.html?source=rss&url=http://www.infoworld.com/article/05/10/07/41OPsecadvise_1.html.
- **The Four Most Dangerous Security Myths:** Network security is all about nightmares.The four more dangerous security myths are: patches always fix the security hole; SSL is secure; Theoretical vulnerabilities don't pose a danger: and Wireless networks are inherently insecure. Source: http://www.networkingpipeline.com/handson/171204280.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
3	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
4	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
5	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
6	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
7	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
8	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
9	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
10	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.

Table updated October 10, 2005

[back to top]

Last updated October 13, 2005